IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEVADA

EVERETT BLOOM; JACK GRAHAM; and DAVE LINHOLM, on behalf of themselves, and those similarly situated,

Plaintiffs,

v.

ZUFFA, LLC; ENDEAVOR STREAMING, LLC; and ENDDEAVOR GROUP HOLDINGS, INC.

Defendants

§ § § § § § § § § §

Civil Action No. 2:22-cv-00412-RFB-BNW

REPLY EXPERT REPORT OF REBECCA HEROLD JANUARY 29, 2024

FILED UNDER SEAL

CONTAINS MATERIAL DESIGNATED

HIGHLY CONFIDENTIAL – ATTORNEYS EYES ONLY

TABLE OF CONTENTS

I. INTRODUCTION

1. I submit this rebuttal report to reply to testimony submitted by Ron Schnell in connection with Zuffa LLC's Response to Plaintiffs' Motion to Certify Class in the above-captioned matter. I incorporate the entirety of my opening report as necessary with regard to the terms of my engagement and reimbursement. I have read and relied upon the additional documents cited in this Reply report.

2. In my opening declaration, I opined that there is common evidence that could be applied on a classwide basis to determine if Defendants sent personally-identifiable information regarding its users' video views to Meta Platforms, Inc. ("Meta"). I identified multiple pieces of common evidence that could be applied to this question, including the following:

REDACTED

[redacted]

[redacted]

REDACTED

REDACTED [redacted]

[redacted]

REDACTED [redacted]

[redacted]

REDACTED [redacted]

[1] My opening report erroneously identified the year Zuffa placed the video titles back into the URLs as 2021. The correct date and year is October 1, 2020.

REDACTED

3. In his declaration, Mr. Schnell incorrectly describes how key technologies discussed in my declaration work in order to obfuscate the effects of Zuffa's actions, disclaim Zuffa's responsibility, and impugn my knowledge and expertise.

4. I stand by my analysis based on my education and my 30+ years of experience in the IT field as a systems engineer, with a focus on architecting websites, implementing security protections and privacy controls, as well as my experience teaching and creating curriculum for Master's degree students in that same field for 9 ½ years at an NSA accredited institution.

5. Contrary to Mr. Schnell's testimony, there is no reasonable dispute that there Zuffa caused the alleged data transmissions. The fact that they occurred via users' computers is immaterial; the software code that executed the transmissions did so because Zuffa configured its web pages to download a Meta Pixel to the users' computers when they navigated to ufcfightpass.com web pages. REDACTED

6. Mr. Schnell's statement that is it impossible for Zuffa to know what was sent to Meta is false. Every organization that has a website is responsible for knowing everything that their own website is doing, including collecting and sharing data. My own examination of the ufcfightpass.com web page (as well as the investigation that led to the Complaint in this action) shows that it is possible to see what cookies are being sent and what data they contain. While this is circumstantial, rather than direct, evidence that Meta receives the cookie data

being transmitted, it is nonetheless relevant evidence that a diligent web site operator could have obtained. Furthermore, the Meta Developers Documentation details the activities that will occur for the associated code, thereby providing notice of what will be disclosed. On top of that, a multitude of academic studies provided notice of specific data transmitted by the Meta pixel, including URLs and Facebook IDs. REDACTED

7. Mr. Schnell is also incorrect when he states that certain data sent to Facebook were not personally identifying information (PII) data. Specifically, despite Mr. Schnell's assertions, it is well-established that unique identification of a user's computer allows the user to be personally identified. Below, I provide additional facts and examples to support that the types of data discussed in my declaration (such as _fbp parameter) are PII.

8. Contrary to Mr. Schnell's assertions, I never stated that all visits to ufcfightpass.com would inevitably lead to disclosures of PII. My testimony just described a computer system that is common to all of Zuffa's web pages, that was configured during the relevant period to disclose Facebook IDs and video titles. Nothing in Mr. Schnell's declaration rebuts my actual testimony. To the extent Mr. Schnell testifies that facts specific to individual computers could have prevented the default settings of Zuffa's web page code from operating to share user PII via cookies, he fails to present any evidence that those circumstances occur frequently enough to dominate the common evidence embodied in the system defaults. REDACTED

9. Mr. Schnell also provided a wide range of statements within his rebuttal that were factually incorrect, including his characterizations of my deposition testimony REDACTED

a. For example, he falsely stated that I misidentify Zuffa as the creator of third party cookies, REDACTED

REDACTED

d. These and other falsehoods show that Mr. Schnell's testimony is factually inaccurate and unreliable.

II. BY INCORPORATING THE META PIXEL INTO ITS WEBSITE, ZUFFA CAUSED THE ALLEGED SHARING OF PII WITH META

10. As discussed briefly above, Mr. Schnell incorrectly states that Meta caused the transmission of users' information to Meta, such that Zuffa had no role at all in the data sharing.

11. Mr. Schnell's comments demonstrate a lack of understanding for business accountability for the websites they make available to their customers and the general public, and the associated actions of the business. Organizations that provide websites are accountable for the actions

their websites perform or allow. This includes having websites that were breached because of vulnerabilities in how the site was coded and engineered, and also for how the data collected by websites were used and shared with others. This is not a new concept; it is a longstanding tradition. Even when contractors are hired by a business to create, maintain or support a website for them, the contracting business is responsible for the activities and actions taken by the contractors, who are doing business on their behalf. Zuffa is responsible for the Meta Pixels that Zuffa placed into the code of their Zuffa website pages, so they are the ultimate cause of the unconsented sharing of PII through their website web pages' code.

12. Mr. Schnell's assertion that Zuffa played no role in causing the alleged transmissions of PII also displays a specious understanding of causation. While it may be true that the digital cookie transmission was sent from users' computers, the fact is that the code being run on the users' computers to display Zuffa's web pages was written by Zuffa and loaded onto the users' computers from servers controlled by Zuffa. And though the pixel code may have been written by Meta, Zuffa placed that code into its website pages.

REDACTED

III. Personally identifiable information (PII) includes the data in cookies, Meta Pixels and other types of online tracking tools

15. In his paragraph 50, Mr. Schnell writes,

> "*Ms. Herold appears to not understand that the contents of the _fbp cookie do not contain personally identifiable information such as a Facebook ID*."

As explained in multiple paragraphs within my declaration, and throughout this rebuttal report, data that can be associated with a specific individual is considered to be personally identifiable information (PII) because it can be, and is, associated with a specific individual.

16. Based upon the incorrect statements made throughout his rebuttal report, Mr. Schnell clearly does not understand digital cookies or how they are associated with specific individuals and the privacy impacts and harms they can cause to those individuals. Throughout the history of using digital cookies within browsers, the entire purpose of the cookie has been to associate an individual using a specific computing device with the computing device's browser. A cookie is a small file stored in the computing device user's hard drive or in the browser, depending on the associated operating system and the browser used. A cookie can contain any type of data that the business responsible for the website decides to include within it, including the webpage visited and associated data and activities, such as the name of specific videos viewed.

17. During the period under consideration for the case, up through at least May, 2023, the Zuffa website demonstrably was collecting and transmitting the names of the videos viewed to Facebook/Meta through the use of third-party cookies. My screenshots taken and included in my Declaration includes this evidence. Zuffa employees and contracted workers could have easily removed cookies, or replaced them with other cookies and other types of tracking technologies after that timeframe. First-party cookies are also used by the website itself to track the videos Zuffa subscribers are viewing, which can then be shared with third parties through technologies other than cookies.

18. Zuffa is responsible and accountable for knowing about, having oversight for, and making changes for all the code on their website. To claim they are not responsible for the code on their site is not only incorrect, it is illogical. The FTC, FCC, and other regulatory agencies have applied fines and other penalties against hundreds of organizations for the personal data collection from their websites and associated actions. For example,

    a. In 2019 the FTC reached a settlement with Facebook, Inc. who agreed to pay a $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users' privacy, to settle Federal Trade Commission charges that the company deceived their users about their ability to control the privacy of their personal information[2].

    b. In 2019 the FTC reached a settlement with Google and YouTube, who agreed to pay $170 million to settle allegations by the Federal Trade Commission and the New York Attorney General that the YouTube video sharing service illegally collected through the use of their website personal information from children without their parents' consent.

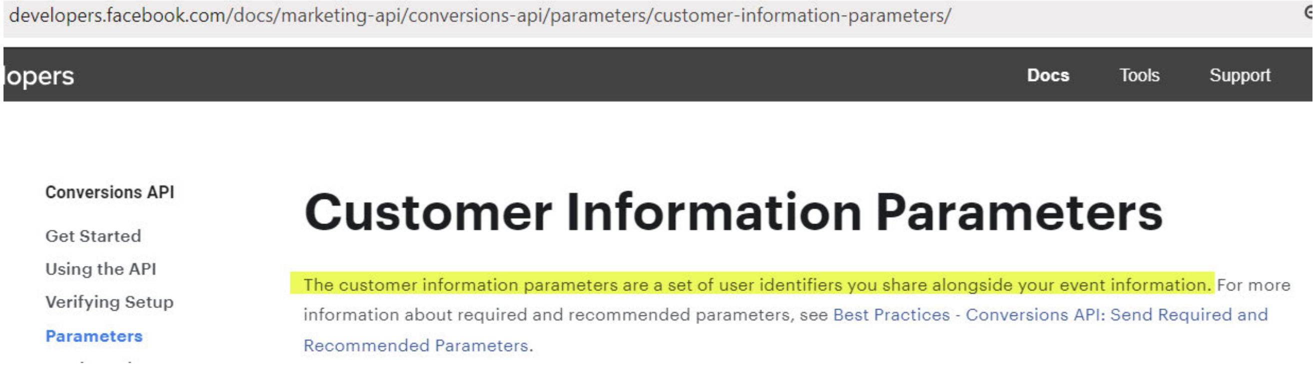
19. The organization providing the website where the cookies are placed on website visitors' computing devices has complete control over putting cookies into the computing devices of their website visitors. If they claim to not know the cookies that are being used on their website, they are either irresponsible and negligent in managing their website, or they are being deceptive and dishonest in how they described how their website tracks visitors and subscribers.

20. The Meta Developers Documentation website clearly explains the purpose of the _fbp cookie, and provides a list of what they explicitly call, "user_data" parameters[3]. Facebook explicitly

[2] See https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

[3] See the, "Customer Information Parameters" page in the "Meta for Developers" website, provided by Facebook, at https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/

includes fbp as one of the types of "user_data" that can be associated with specific individuals. Even the URL indicates this is information for targeted marketing, which is explicitly used to track specific individuals who meet specific characteristics, such as watching specific videos. Mr. Schnell's statements either demonstrate he has a complete lack of familiarity and understanding for how the Meta Pixel works, or he is being purposefully deceptive.



developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/

Customer Information Parameters

The customer information parameters are a set of user identifiers you share alongside your event information. For more information about required and recommended parameters, see Best Practices - Conversions API: Send Required and Recommended Parameters.

Source: Meta for Developers website; https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/. With additional information from the full Developer Documentation; https://developers.facebook.com.

21. Mr. Schnell's claims that fbp is not PII, when all the other "user_data parameters" Facebook lists are clearly PII data, is not logical; this claim is incorrect. A primary purpose of cookies is to track activities of specific individuals and then target them with marketing messages based upon their online activities, such as watching specific UFC Fight videos. The Meta for Developers documentation explains this multiple times on their website, and in many different ways.

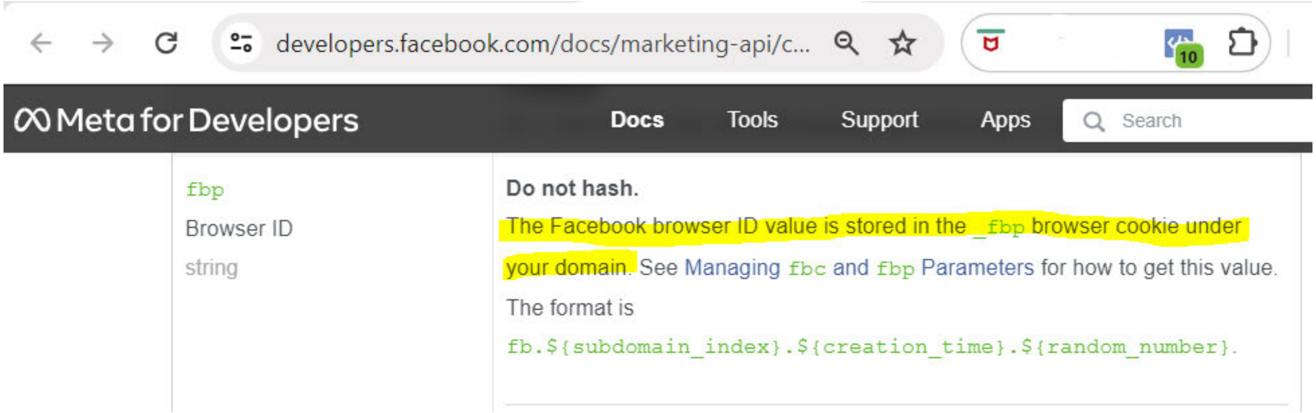
22. The following is the list of all the "user_data parameters" descriptions Facebook lists for their Meta Pixel developers to use on their own associated websites[4]. These are all PII data items that can be used to associate with a specific individual user.

    a. Email
    b. Phone Number

[4] Ibid.

c. First Name
d. Last Name
e. Date of Birth
f. Gender
g. City
h. State
i. Zip Code
j. Country
k. External ID: "Any unique ID from the advertiser, such as loyalty membership IDs, user IDs, and external cookie IDs. You can send one or more external IDs for a given event."
l. Client IP Address
m. Client User Agent: The browser being used.
n. Click ID: This logs the subdomain, creation time, and query value, providing insights to the context of the activities, and what the user is doing at a particular webpage.
o. Browser ID: This is the fbp parameter for the _fbp cookie, described in the next paragraph.
p. Subscription ID
q. Facebook Login ID
r. Lead ID: This associates the specific user to a lead…a person to target market.
s. anon_id: Used only for app events
t. madid: The advertising ID for an Android device, or the Advertising Identifier (IDFA) for an Apple device.

23. Indeed, the "Customer Information Parameters" page in the "Meta for Developers" website, provided by Facebook, explicitly states that the _fbp cookie contains the Facebook browser ID. Here is a screenshot directly from the developer's guide provided for developers to use, including the Zuffa website developers, who would have, and should have, known the purpose and use of each of these customer information parameters. This is explicitly stating that the visitors to webpages where these cookies are set contain the associated user's Facebook browser ID (this is PII), and it is under the developer's domain, in this case the Zuffa domain.



fbp
Browser ID
string

Do not hash.

The Facebook browser ID value is stored in the `_fbp` browser cookie under your domain. See Managing `fbc` and `fbp` Parameters for how to get this value.

The format is `fb.${subdomain_index}.${creation_time}.${random_number}`.

24. Mr. Schnell's statements indicate that he does not have an understanding of the type of data that can be considered as PII. Simply put, any data that can be associated with a specific individual, location where individuals reside or known to otherwise be unique to an individual, such a specific computing device, can and has been considered to be PII for many decades.

25. All the data items that are used to identify individuals are considered to be types of personal data. Within the context of tracking the online activities of individuals, a wide range of data items, including all those listed as "user data parameters" are personally identifiable information (PII) either explicitly, such as name or c_user, as well as probabilistically, such as IP addresses and browser IDs. For example, IP addresses are used to determine such personal characteristics about the associated individual as the approximate user location such as city and zip code, identify the associated user's internet service provider's name, and log internet activity within a session. An IP address is similar to a social security number in the way in which it is assigned to an individual computer each time it accesses the internet, identifying the computer and allowing for the interaction of the servers and computers to communicate across platforms. Even though the IP address doesn't explicitly reveal a person's name, it does reveal pieces of personal data that anyone with a little know-how can access.

26. Mr. Schnell also demonstrates he has no clear background in security or privacy. He uses the terms "identified" and "identifiable" interchangeably (see ¶ 50). "FBP is not identifiable" is a

false statement. The Facebook Developers Documentation clearly indicates it is user data that supports tracking the online activities of specific individuals.

27. The U.S. Health Insurance Portability and Accountability Act (HIPAA) establishes that internet protocol (IP) addresses (which every type of computing device and smartphone uses to connect to the internet) are types of protected health information (PHI). PHI is a sub-set of personally identifiable information.

28. The U.S. Federal Trade Commission (FTC) has taken a statutory position that identifiers of a user's computing device are types of "personal information," another term commonly used to mean "personally identifiable" information[5].

29. Mr. Schnell's comments and statements also demonstrate that he does not understand that PII data can be deterministic to an explicit individual, (e.g., c_user) or probabilistic based upon the context of the situation (e.g., _fpb). Given these ways in which PII data have been established and recognized throughout the years, other data fields used by Zuffa, such as User_agent, IP address, and _fbp can be considered to be unique identifiers.

IV. Mr. Schnell's "REASONS WHY USERS MIGHT NOT HAVE FACEBOOK COOKIES" Are Uncommon and Moot in View of Meta's Pixel Data

30. In his report, Mr. Schnell accuses me of failing to take into account the possibility that Facebook cookies will not be present on the user's computer. Schnell Decl., ¶ 45.

31. Among the reasons he accuses me of failing to take into account are the possibility that the user's browser was one that blocked third-party cookies. Mr. Schnell is incorrect. I identified the possibility that browsers could block third-party cookies. See Herold Decl., ¶ 25. However, it is my opinion that the most common fact pattern would involve Chrome, the most

[5] For example, see the Children's Online Privacy Protection Act (COPPA), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312, which defines "personal information" as including, "A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."

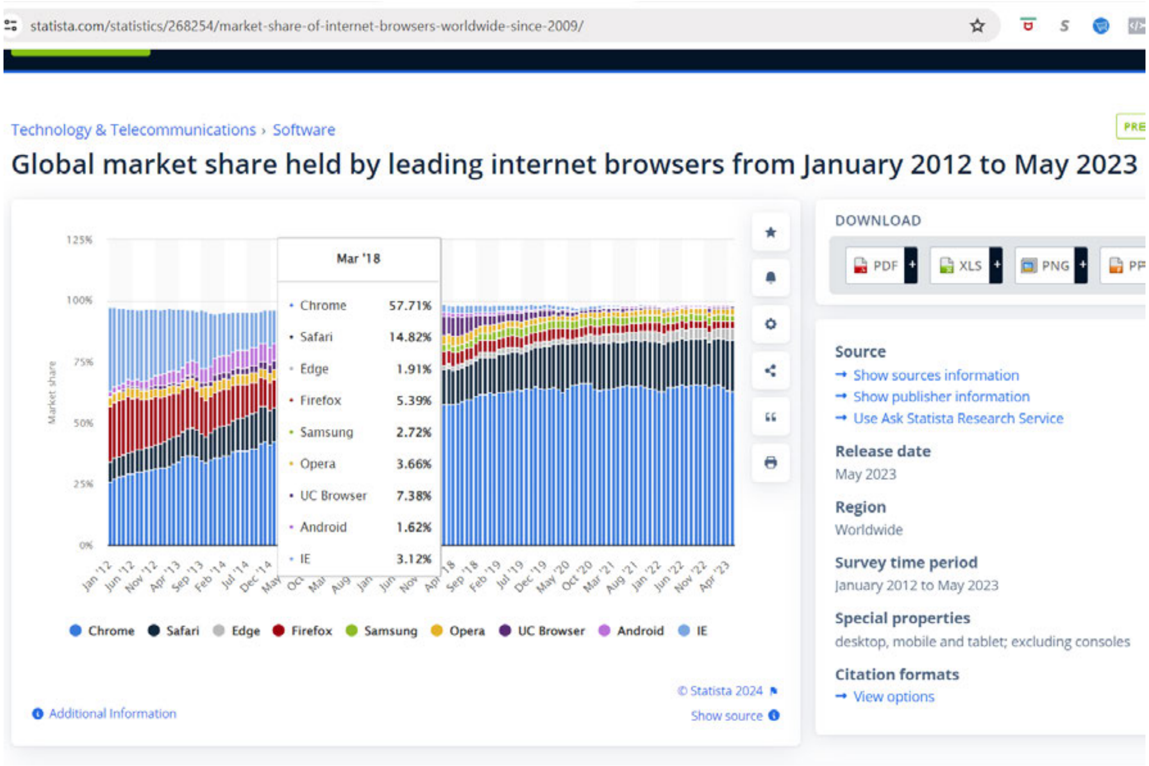
commonly-used browser during the period in question, without any cookie-blocking settings utilized.

32. Mr. Schnell does not dispute that, during the period from March 4, 2018 to June 3, 2022, Chrome was the most commonly-used browser in the United States. In fact, Mr. Schnell provided no evidence at all regarding the frequency with which other browsers are used.

33. In their Opposition brief, Defendants presented non-expert evidence that Safari and Firefox comprise up to 30% of the U.S. desktop browser market, and that Safari comprises up to 50% of the mobile browser market. Even assuming Defendants' market share statistics are accurate, Chrome represents approximately 70% of the U.S. desktop browser market and roughly 50% of the mobile browser market.

34. In reply to the above assertions from Mr. Schnell and Zuffa, I note that studies of U.S. browser use indicate that most UFC Fight Pass website users would have used Chrome browsers.

35. As stated in my deposition, the preponderance of online users, anywhere from 60% - 75%, used Chrome browsers. The images below provide Chrome usage reported by Statista. Use of Chrome browsers in the U.S. increased from the clear majority (57.7%) of the population in March, 2018, to an even larger preponderance of the population (66%) in June of 2022.



statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/

Technology & Telecommunications › Software

Global market share held by leading internet browsers from January 2012 to May 2023

Mar '18	
Chrome	57.71%
Safari	14.82%
Edge	1.91%
Firefox	5.39%
Samsung	2.72%
Opera	3.66%
UC Browser	7.38%
Android	1.62%
IE	3.12%

DOWNLOAD

Source
→ Show sources information
→ Show publisher information
→ Use Ask Statista Research Service

Release date
May 2023

Region
Worldwide

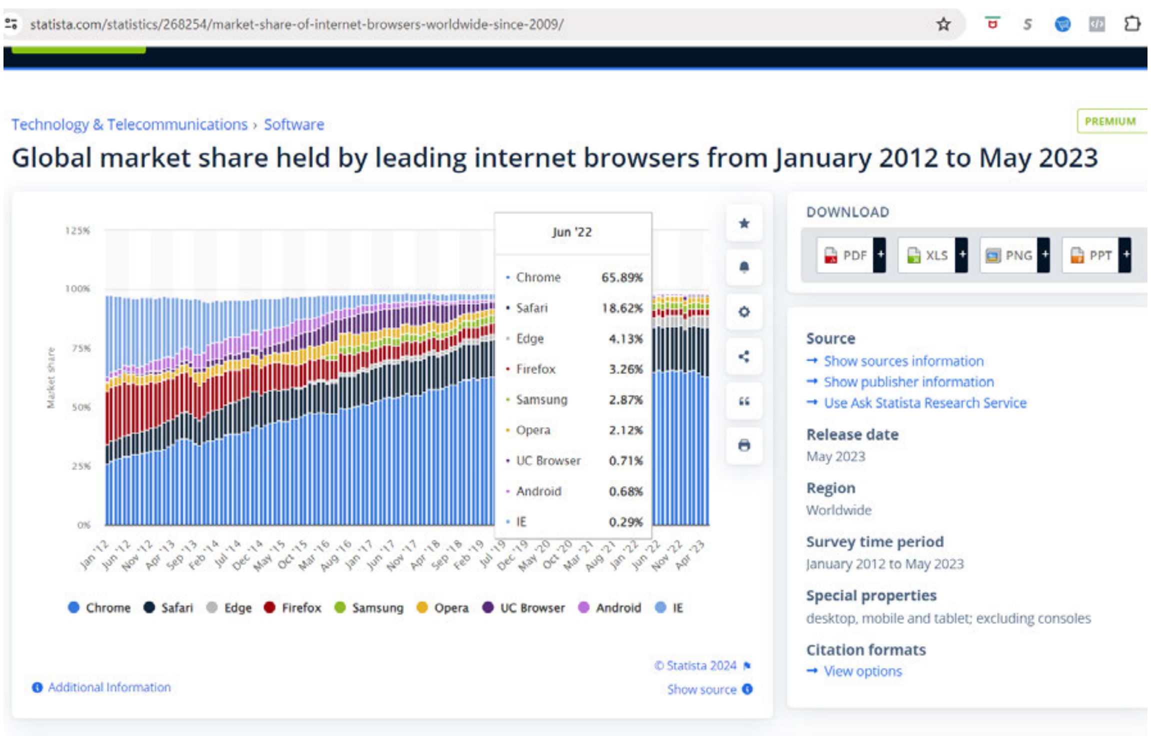
Survey time period
January 2012 to May 2023

Special properties
desktop, mobile and tablet; excluding consoles

Citation formats
→ View options

© Statista 2024
Show source
Additional Information

Source: Statista.com on January 3, 2024.



statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/

Technology & Telecommunications › Software

Global market share held by leading internet browsers from January 2012 to May 2023

Jun '22	
Chrome	65.89%
Safari	18.62%
Edge	4.13%
Firefox	3.26%
Samsung	2.87%
Opera	2.12%
UC Browser	0.71%
Android	0.68%
IE	0.29%

DOWNLOAD

Source
→ Show sources information
→ Show publisher information
→ Use Ask Statista Research Service

Release date
May 2023

Region
Worldwide

Survey time period
January 2012 to May 2023

Special properties
desktop, mobile and tablet; excluding consoles

Citation formats
→ View options

© Statista 2024
Show source
Additional Information

Source: Statista.com on January 3, 2024.

36. Mr. Schnell also opined that I failed to account for sharing of computers by multiple people. Schnell Decl., ¶ 45. This criticism is inconsequential, because most people do not share their computing devices with others, or do so only rarely. This has resulted in a long-time practice for law enforcement, regulators, and judges to associate a device and associated identifiers as representing specific individuals[6]. Online data, such as IP addresses, "user agent," and other items collected and stored on computing devices that can be associated with specific individuals with a high confidence of probability are deemed personally identifiable information (PII). Such data can, and often is, used to reveal activities such as the videos viewed on specific websites from a computing device and associate that to specific individuals, such as specific subscribers to a website.

37. Mr. Schnell also asserts that I failed to account for people who do not have Facebook cookies on their computers because they have logged out of Facebook. But Mr. Schnell glosses over the fact that "logging out" of Facebook requires explicitly doing so (i.e., clicking "log out"). Merely closing one's browser or a window that has Facebook open will not log out of Facebook, nor delete the c_user cookie. Most internet users do not logout of the sites they are logged into. This practice results in persistent cookies, such as the Facebook c_user cookie, remaining in the sites they have visited, allowing Meta to continue to track those individuals.

38. In my experience with hundreds of clients, I've observed this many times. Not only do they not logout, when they experience a site that forces them to logout, most complain about it.

39. This issue has been written about many times.[7] This widespread habit is one that marketers know well, and have their website administrators take advantage of with regard to how they implement the persistent cookies on their websites.

[6] For example, see https://www.supremecourt.gov/DocketPDF/19/19-8596/144423/20200528192745880_VD.cert.Final.pdf.

[7] Just a couple of examples include: 1) "The impossibility of logging off: The logout button has become practically defunct." April 6, 2023. By Terry Nguyen at https://www.theverge.com/23670169/logout-button-ui-websites-design-ui-interface. 2) "Auto-logout more rigorous - remove auto log-out" https://forum.asana.com/t/auto-logout-more-rigorous-remove-auto-log-out/34861/2

REDACTED [redacted]

41. Mr. Schnell also asserts that I did not take into account people who have no Facebook accounts, and thus no Facebook ID to disclose nor c_user cookie. But Facebook is one of the oldest and largest social media websites in existence, and most people who are active online have a Facebook account. See, e.g., https://thesocialshepherd.com/blog/facebook-statistics#:~:text=The%20U.S.%20population%20currently%20sits,States%20were%20regular%20Facebook%20users (reporting 71% of "internet users" are "regular Facebook users"); https://www.statista.com/topics/5323/facebook-usage-in-the-united-states/#topicOverview (reporting 243M of the United States' population of 350M (69%) have a Facebook account). In any event, this possibility can easily be addressed either by using Meta's pixel data to identify users who were tracked by Meta via their Facebook ID, or by limiting the class to people who had a Facebook account.

42. Mr. Schnell also cites the possibility that users deleted cookies, whether for all sites or just Facebook. But he supplies no evidence this as a frequent occurrence. Indeed, many research reports from the time period associated with this case report that most cookies are not only not blocked but also not deleted from users' computers. A 2020 research report that examined 82,890 unique website visitors using desktops and mobile devices (laptops, smartphones, tablets, and/or other types of mobile devices), found that 70% never to occasionally decline cookies. Only 6.95% used an ad blocker. Only 0.8% of them used blockers on mobile devices

(0.8 %)[8]. For additional examples, see Unesco[9], Kruikemeier.[10] Similar results are provided by many other research report. Online users also often view blocking cookies as blocking their access to information on a site that they are using. "To many of them, the only reasonable option is to provide consent while opting in for an ad-blocker extension or any other tracking blocker in their browser. Since cookie consent prompts always stand in the way of the content, they are often dismissed almost instinctively.[11]"

43. Additionally, even when the small percentage of online users think they are blocking cookies, it is subsequently discovered that the cookies were not blocked[12].

[8] From, "(Un)informed Consent: Studying GDPR Consent Notices in the Field." https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-christine_utz.pdf. 2020.

[9] From "Global Survey on Internet Privacy and Freedom of Expression," at https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000218273&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_718fcd00-7614-41a8-9724-2f1916005a0c%3F_%3D218273eng.pdf&updateUrl=updateUrl9578&ark=/ark:/48223/pf0000218273/PDF/218273eng.pdf.multi&fullScreen=true&locale=en#%5B%7B%22num%22%3A129%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C0%2C694%2Cnull%5D: "Technical implementations of cookies have long evolved beyond the point where users have any meaningful control over being tracked by them. Cookies are often set for years on a user's computer and are extended automatically each time the user visits an associated website. They can also be set by browser add-ons such as the 'Adobe Flash' independently of the main browser. Should a user attempt to remove their cookies from one of the many locations in which they can be stored, they are recreated from other storage areas or using other identification mechanisms such as session IDs, browser add-ons, cookie caching scripts or any number of other methods which allows for cookies to be recreated without the consent of individual users"

[10] Research from Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. Communication Research, 48(7), 953-977. https://doi.org/10.1177/0093650218800915 indicate that 60% of online users never to occasionally delete cookies, and 70% never to occasionally decline cookies.

[11] From, "Privacy UX: Better Cookie Consent Experiences" https://www.smashingmagazine.com/2019/04/privacy-ux-better-cookie-consent-experiences/ April 10, 2019.

[12] For example, "The FTC settled with Google for $22.5 million after its web browser placed advertising tracking cookies on customers' browsers after the company had erroneously informed customers that the default browser settings would block third-party cookies." From "In re the Matter of Google, USA Federal Trade Commission," https://www.ftc.gov/enforcement/cases-proceedings/case-documentsearch?title=google&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/122-3237/google-inc; Trade Regulation Reporter, Google,

V. UFC Fight Pass Website Sent User Identifiable Data and Associated Videos to Meta

44. Mr. Schnell is not correct in how he describes how website information is transmitted to Facebook, which is a subsidiary of Meta. The Zuffa UFC Fight Pass website executes the same code for every website visitor. Mr. Schnell did not provide any evidence that what I provided screenshot evidence of within my June, 2023 Declaration report was incorrect. Instead, he provided a screenshot, lacking details about the context of the view, including the type of browser, and lacking dates for when it was captured. Given that Zuffa has clearly changed their website since my report was submitted in early June, 2023, his argument is invalid. If the evidence has been destroyed after the documented event, collecting a screenshot as an artifact after the website changes removed the evidence does not prove anything other than Zuffa changed the website to remove the cookies and Meta Pixels that were in place during the timeframe when they were collecting PII from their website visitors.

45. Mr. Schnell makes incorrect statements about the types of data the UFC website transmits to Facebook. This demonstrates that Mr. Schnell lacks understanding for how the Meta Pixel works. Refer to my Declaration for a detailed explanation of this. Mr. Schnell did not mention those facts that were provided in his rebuttal.

46. Mr. Schnell's statements within his full rebuttal related to his stated conclusion: "Ms. Herold incorrectly states that Meta (with certainty) is able to use certain parameters to "identify the person associated with [a] computer," is first of all not an accurate quote from my deposition. It also is incorrect to indicate that the data cannot be used to identify an individual, which is explained within this report.

Inc.—Complaint and consent order, FTC Dkt. C-4499, File No. 122 3237," announced September 4, 2014; issued
December 2, 2014, ¶17,178, Federal Trade Commission, as referenced in, "The Internet and Public Policy: Privacy
and Consumer Protection." 2018. https://www.house.mn.gov/hrd/pubs/int_privacy.pdf.

VI. UFC Fight Pass website making disclosures to Meta of personally identifiable data (PII) and associated videos for a preponderance of all Zuffa subscribers

47. Evidence can be applied as common proof, as explained within my June, 2023 Declaration and within this report, that the UFC Fight Pass website was collecting PII and associated videos viewed, as demonstrated by my step-by-step analysis and evidence supporting screenshots, for a preponderance of all Zuffa subscribers, and disclosing that data to Meta.

REDACTED

49. Mr. Schnell's statement made the following illogical statement at paragraph 23:

> "Ms. Herold incorrectly implies that certain actions involving cookies occurred for all users of the UFC Fight Pass website during a certain time frame, while there are myriad scenarios in which certain users would not have these actions occur."

I did not make such a statement. Mr. Schnell is making a false allegation in interjecting statements seemingly to change the meaning of my testimony to better fit his narrative for his client.

50. Mr. Schnell misinterprets my statements. My testimony is that the code for the Zuffa website does not change depending upon different users. Accordingly, that code can be applied as common evidence for all users. I do not deny that individual variations from uses' computers could alter the results on occasion, though I continue to believe most of those individual variations (e.g., cookie clearing, cookie blocking, adjusting Facebook and browser settings) are infrequent relative to population of UFC subscribers as a whole.

VII. Tracking technologies Zuffa implemented on the Fight Pass website sent personally identifiable data and associated videos to Meta

51. Mr. Schnell made the following statement at paragraph 24:

REDACTED

REDACTED

[redacted]

REDACTED

[redacted]

REDACTED

[redacted]

[redacted]

REDACTED

[redacted]

REDACTED

[redacted]

REDACTED

[redacted]

REDACTED

[redacted]

[redacted]

REDACTED

[redacted]

[redacted]

[redacted]

[redacted]

REDACTED

[redacted]

[redacted]?

REDACTED

REDACTED [redacted]

[redacted]

58. Mr. Schnell indicated the following in ¶22:

> ***Ms. Herold incorrectly states that Meta (with certainty) is able to use certain parameters to "identify the person associated with [a] computer."***

Mr. Schnell is not only incorrect with regard to his statement that the Meta user_data parameters cannot identify the individual associated with a computing device, but he also modified what he represented as a verbatim quote from my Deposition, which is dishonest and calls to question his other similar types of statements.

59. Mr. Schnell is correct that I indicated certain data items can identify individuals that used a specific computing device. Numerous decisions and convictions have occurred over the past several decades based upon computer data. I provided evidence and explanation in my Declaration and in this report that such data is and has been used and considered to be basically certain identification.

60. Mr. Schnell indicated the following at ¶23:

> **23. Ms. Herold incorrectly implies that certain actions involving cookies occurred for all users of the UFC Fight Pass website during a certain time frame, while there are myriad scenarios in which certain users would not have these actions occur.**

61. Organizations that provide websites configure them with computer code that executes in the same manner for every website visitor. Such code is created to fulfill the goals of the organization, such as to collect specific types of data from website visitors, to set cookies in

website visitors' browsers, and other actions. The intent of the organization for all website visitors is demonstrated by code. While tools such as cookie blockers are available for website visitors to use, the information I provided in ¶42 and ¶43 demonstrate that a very small percentage of online users utilize cookie blockers. Also, as I testified in my deposition a statistically tiny percentage (0.05%) of all online users utilize the Brave "privacy" browser (which is not 100% effective anyway; no similar tools are), and given that the average number of computing devices per person in the U.S. was 8.2 in 2018, increasing to 13.4 in 2023[13], the likelihood of a Zuffa website viewer using a computing device that has cookies that the Zuffa website code placed on at least one of their browsers is very high. However, regardless of the browsers used, the intent of Zuffa to place cookies within the browsers of their website visitors is demonstrated through the same code that executes for each person who visits their website. This is the one constant scenario that does not change.

REDACTED

[redacted]

[redacted]

[redacted]

[13] See, "Average number devices and connections per person worldwide in 2018 and 2023". Statista. https://www.statista.com/statistics/1190270/number-of-devices-and-connections-per-person-worldwide/

REDACTED

[redacted]

REDACTED

REDACTED

64. Mr. Schnell made the following claim in ¶30. Mr. Schnell's statement is incorrect. Cookies are usually transmitted in browser headers, or can be established in javascript.

> Schnell's ¶30:
>
> ***30. When a website wants to use cookies, there is special source code on the page that tells the browser that it will be storing a cookie. This cookie can contain any information the website desires. It could be something simple like a bookmark, so that the next time that browser goes to the page it can start where it left off. Or it can be much more complicated, storing all sorts of preferences.***

65. In ¶ 33 of his declaration, Mr. Schnell arbitrarily ties together two unrelated statements to create the impression that I testified Zuffa transmitted c_user cookie data to Meta using Zuffa's servers. But the first statement he quotes, from ¶ 5 of my declaration in support of the motion for class certification, is simply that "Zuffa web pages had code that tracked the URLs each subscriber accessed and sent that data to Meta." While this statement utilized shorthand by referring to code executed on user's browsers in response to navigating to Zuffa's URLs as Zuffa code that sent URLs to Meta, there is nothing inherently incorrect in my description.

66. Mr. Schnell then tries to create a strawman of my argument by tying truncated, out of context deposition testimony regarding my identification of the c_user and m_page_voice cookies as evidence of data transmission to Facebook back to my declaration statement. But his characterization distorts my testimony and takes it out of context. Mr. Schnell omits the end of my response to the question, in which I note that "it follows that that's as described being sent on to Facebook. That was from the developer. That was the whole purpose of that code." In context, I was clearly answering the question of how I knew the data was being sent to Meta, not identifying whether Zuffa's servers transmitted the cookies.

67. Mr. Schnell goes on to state in ¶33 that "UFC has no visibility" into transmission of third party cookies. While it is technically true that Zuffa cannot "see" the data transmission as it is

occurring, Mr. Schnell is being disingenuous, at best, when he says that Zuffa has "no visibility" into data transmission involving third party cookies. Zuffa integrated the Meta pixel into its web site, and Zuffa did so because it knew that Meta would track activity by users. Furthermore, Zuffa could have examined what third party cookies the Meta pixel transmitted by doing quality assurance testing. So even if Zuffa can't read the exact values being transmitted, it should know what it asked Meta to track.

68. At ¶34 of his report, Mr. Schnell falsely asserts that I "suggest[] that Zuffa creates these third party cookies." I am fully aware that Zuffa does not create third party cookies. Mr. Schnell not only misrepresents my testimony, but intentionally omits testimony that contradicts his characterization of my beliefs. In my opening report, I defined third party cookies as cookies "created and owned by someone other than the web site a user is viewing." Herold Decl., ¶ 33. And in the deposition, I testified unequivocally that Meta, not Zuffa, created the c_user and m_page_voice cookies. See Herold Deposition at 153:4-8 ("Q. [A]re you saying that the Zuffa site created the c_user and m_page_voice cookies? A. . . . They [i.e., Zuffa] did not create them [i.e., the c_user and m_page_voice cookies]. . . . Q. How are the c_user and m_page_voice cookies created? A. Through the Meta pixel"). .

69. Mr. Schnell also criticizes me, in ¶ 35 of his report, for relying on the presence of the c_user cookie in my browser while viewing a ufcfightpass.com web page as evidence Zuffa knew I was a Facebook user. I concede that my testimony was not clear. What I meant to say that Zuffa could have confirmed transmission of the c_user cookie for Fight Pass subscribers who were also Facebook subscribers by having a Zuffa employee who had a Facebook account do the same test I did. And to the extent I testified Meta had "access" to the cookie, I was referring to the Zuffa website code having "access" to the c_user cookie to send it to Meta in the header data as part of the Pixel's GET request to Meta. REDACTED [redacted]

REDACTED [redacted]

REDACTED [redacted]

71. In paragraph 37 of his report, Mr. Schell criticizes ¶ 83 of my report, where I refer to Facebook ID and URLs being transmitted in pixel data. I admit ¶ 85 contains an error; it should have referred to the _fbp cookie, not the Facebook ID. However, the _fbp cookie is, contrary to Mr. Schnell's testimony, a unique identifier, at least within Facebook. That is because the _fbp cookie can be associated with a Facebook ID if pixel event data connects those two identifiers. REDACTED [redacted]

72. Mr. Schnell wrote in his ¶40 that my statements that the UFC Fight Pass website transmits cookies and that Zuffa has control over these transmissions were incorrect:

> 40. However, Ms. Herold incorrectly implies that:
>
> a. These cookies are transmitted by the UFC Fight Pass website to Meta,

b. The UFC Fight Pass website had control over the transmission
of these
cookies from the user to Meta, and
c. That the UFC Fight Pass website causes these cookies to be
placed on the
browser.

73. Mr. Schnell is wrong, and does not seem to understand how a business establishes their website and makes their own decisions about how the websites for which they are responsible work. As discussed above, "website" refers to the code Zuffa writes, or obtains from other code writers, and downloads to user's computers. That code, over which Zuffa had control, transmits cookies.

74. In that same paragraph, Mr. Schnell misstates that I implied the UFC Fight Pass website created the Meta cookies to be placed on the user's browser. I defined third party cookies in my report as those created by a third party website. I also testified that it was Meta, not UFC, that created the cookies.

75. Mr. Schnell wrote the following in his report ¶41. Mr. Schnell is incorrect, and does not demonstrate an understanding of how cookies work.

> **41. As described supra, the UFC Fight Pass website cannot access cookies that were placed by Facebook.com on users' browsers, so they cannot transmit the contents of those cookies to Meta or anyone else. The UFC Fight Pass website also has no visibility into these cookies, the contents of these cookies, what other websites running on users' browsers, or any users' browser settings.**

REDACTED

[redacted] The second sentence is misleading, because it implies that it is impossible for Zuffa to quality assurance testing of what data its website can transmit, when Mr. Schnell himself testified that he could see what data was being transmitted by his browser.

76. Mr. Schnell wrote the following in his report ¶42. Mr. Schnell is wrong. Zuffa has complete control over their own website, and how it works and is configured. Once more Mr. Schnell is demonstrating his lack of understanding for how businesses are responsible for their own websites and how they work. Zuffa controls and makes the decisions for, the code running on their website, including for transmission of any cookies from their website. Zuffa is responsible for knowing how the third-party cookies will be used by the associated entities that own the cookies; Zuffa is enabling the use, or misuse, of the data within these cookies by sending them to Meta.

> **42. When the contents of these cookies (to the extent they existed) got transmitted to Meta, it was because Meta causes them to be transmitted, and the UFC Fight Pass website had no control over how Meta conducts their business, nor can they tell in advance what Meta will do with its own cookies.**

77. Mr. Schnell wrote the following in his report ¶43. Mr. Schnell is wrong, and demonstrates his lack of understanding for how cookies work.

> **43. Specifically, when a user's browser is communicating with Facebook.com, the Facebook.com website decides when it is time to use one of its cookies, such as c_user. Depending on what framework Facebook is using at the time (something that Ms. Herold cannot know), Facebook.com will cause the browser to execute specific code to request the value of the cookie from the browser's storage. For example, Facebook.com might cause the user's browser to execute the following code (or something similar):**
>
> **c_user = Cooke.get_cookies(req)["c_user"]**

Mr. Schnell's code example is nonsense. The cookies are sent as part of a header in a GET request transmitted by Zuffa's code. Assuming no cookie blocking is in place, all cookies included by Zuffa's GET request will automatically be sent every time.

78. Mr. Schnell wrote the following in his report ¶45.

> **45. It is also important to note that it is a subset of visitors to the UFC Fight Pass website that will have on their browser (and thus transmit) Meta third-party cookies at all. There are several reasons why users might not have had these cookies, including, but not limited to:**
>
> **a. The user might be using multiple browsers or devices, and may not have**

> **been simultaneously logged into Facebook at the same time as they were viewing a video-ondemand on the Fight Pass website on the same browser and same device,**
> **b. The user might not have been a Facebook subscriber,**
> **c. The cookie containing information about a logged-in Facebook account might be for someone else sharing the same device, creating a misattribution to another Facebook user.**
> **d. The user might have been using a browser or device from which they were not logged in to Facebook, or the user might have logged out of Facebook,**
> **e. The user's browser might have been blocking third-party cookies, either by default, through settings, or by extensions, such as ad blockers,**
> **f. The user might have been using a device, such as a Roku or similar,**
> **g. The user's browser might have been in "incognito" mode, or similar,**
> **h. Facebook settings, including "Off-Facebook activity" and other ad settings might have caused data collection to be disabled on their Facebook account,**
> **i. The user might have deleted the cookie manually from their web browser,**
> **j. The user might have deleted all cookies from Facebook.com,**
> **k. The user might have deleted all cookies, or**
> **l. The cookie may have expired.**

As discussed earlier, Mr. Schnell's laundry list of reasons is overblown. Many of the above circumstances are uncommon or even rare (e.g., not being a Facebook subscriber, using incognito mode, deleting all cookies or even just those from Facebook on a daily basis, hitting the "logout" button on Facebook, use of cookie blockers). Others are unlikely to have prevented all data transmission (e.g., cookie expiration, use of browsers or software that block third party cookies). I am informed by Counsel that others (e.g., use of Roku or similar devices, use of non-Chrome browsers) either are excluded or could be excluded from the proposed class,. And for some, Mr. Schnell is just wrong (e.g., Off-Facebook Activity and Targeted Ad settings, REDACTED

79. Mr. Schnell made the following incorrect statement in his report ¶51. Mr. Schnell is incorrect, and demonstrates his lack of experience and understanding of privacy issues, and about how data can be identifiable to a specific individual.

Schnell report:

> **51. In her deposition, Ms. Herold stated, "So, yes, the fbp is part of the [C]onversions API to send data to Facebook through the [_fbp] cookie." I discuss infra why the Conversions API part of this testimony is incorrect. That notwithstanding, the testimony also implies that the _fbp cookie contains data that are personally identifiable information. As I (and the Meta documentation included in Ms. Herold's Declaration) explain, the _fbp cookie contains nothing more than a random number and the time of day (and the characters "fb.1", which are the same for all users).**

To be clear, I am aware what information is contained in the fbp cookie, as I set that out in my report. But I am also aware that he fbp cookie is personally-identifiable in practice because Meta can associate it with other unique identifiers for a user. REDACTED [redacted]. Thus, while the fbp_cookie standing alone may not contain PII, it can be a unique identifier that makes other information it is transmitted with PII as I broadly understand that term.

80. At ¶¶ 56-58 of his declaration, Mr. Schnell incorrectly accuses me of not understanding how the _fbp cookie is generated and whether it identifies me or my device. He is wrong on both counts. First, I was explicit in identifying how the _fbp cookie is generated. See Herold Decl. at ¶¶ 44 & 65. Second, to the extent I used the word "me" in discussing the _fbp cookie, my description is accurate because I was discussing Meta's use of the _fbp cookie as a probabilistic identifier (i.e., one that uses cross-referencing of data to identify the user). While I am informed that some Courts have held that the VPPA does not cover identification based on non-public data, people within the field of computer privacy recognize this as a form of personal identification. In other contexts, regulators, courts, and law enforcement consider computing devices to be directly associated with the individual that owns them, and thus attributable to the individual.

> **56. In her Declaration, Ms. Herold goes back and forth opining that the _fbp cookie is either specific to her (individually), or to her device.**
>
> **57. In paragraph 65, Ms. Herold states, "The Pixel also shows an 'fbp' parameter was created to be specific with me and my visiting this page…the fbp parameter is populated with data from the '_fbp cookie'.19 (9 Herold Declaration at ⁋ 65)**

> **58. Later in paragraph 70, Ms. Herold states, "…As discussed above/below, the _fbp cookie contains a unique identifier for my computer, which Facebook uses to identify the person associated with that computer."20 (20 Herold Declaration at ⁋70.)**

81. Mr. Schnell makes the following statement at ¶59 of his declaration:

> Ms. Herold's description in paragraph 70 is closer to correct, but still not technically accurate. The random number in the _fbp cookie will not change if you are using the same computer, the same browser, and that cookie on that computer and browser has not expired, or otherwise been deleted or blocked. If any of those circumstances are true, the _fbp cookie will contain a completely different time and random number, because a new one will be created.

82. To the extent Mr. Schnell suggests that I testified the _fbp cookie value can never change, I note that I made no such statement.

83. Furthermore, while Mr. Schnell's description of the circumstances under which a new _fbp cookie will be generated is technically accurate, it is also irrelevant as a practical matter. REDACTED [redacted]

84. At ¶ 62 of his Declaration, Mr. Schnell states, "I do not think it is appropriate for a scientific expert to rely on inference from the stated purpose of a technical element from documentation, as opposed to using scientific methodology." This statement is ridiculous. Mr. Schnell is claiming that it is improper to infer Meta's software operates as described in the documentation Meta wrote and distributed to users. Meta's user manuals and related documentation provide the technical specifications and instructions for how to use its technology. Developers use these materials to implement Facebook's code on their web sites. Facebook's documentation defines all terms and parameters used. These documents are absolutely relevant, and there is nothing improper about using Meta's documentation as evidence of how its software works.

85. Additionally, competent software developers would recognize Meta's documents as relevant notification of what information would be disclosed to Meta by use of the Meta pixel. Thus, to the extent Meta's documentation includes descriptions of collection of PII, the documentation is common evidence that Zuffa knew or should have known that it was collecting and sharing PII data with Meta. It is also evidence that Zuffa purposefully used the Meta pixel and Conversions API to track its users' activities for the purpose of targeting them for marketing.

> **62. I do not think it is appropriate for a scientific expert to rely on inference from the stated purpose of a technical element from documentation, as opposed to using scientific methodology.**

86. Mr. Schnell makes the following statement at ¶66.

> **66. However, Ms. Herold's assumption that the _fbp cookie is only used along with CAPI is incorrect. The _fbp cookie can be used with CAPI, but can also be used without it.**

I never made such a statement, and certainly have no such assumption. Mr. Schnell is making unfounded claims. My report did not say anywhere that fbp is used by CAPI exclusively. I also did not make this statement during the Deposition.

87. Mr. Schnell makes the following statement at ¶73 a, b, d2, e.

> **73. Beginning with paragraph 12(e), I would suggest the following corrections to Ms. Herold's step-by-step description, as pertains to the Facebook.com cookies:**
>
> **a. 12(e)(a) states, "At all relevant times, the Meta Pixel caused the user's browser to load the c_user and m_page_voice cookies (both of which are third-party Facebook.com cookies) to load [sic]. These cookies each contain the user's Facebook ID." This is not true, as shown supra, in my description of why only a subset of visitors will have Facebook cookies at all. Ms. Herold's "Step 5" implies that this will always be the case.**

Mr. Schnell misunderstood my statement. "At all relevant times" was meant to refer to the fact that Zuffa's website had a configuration designed to transmit the cookies by default if possible across the entire class period, not that it was 100% effective in doing so.

> **b. An additional inaccuracy in 12(e)(a) is that the Meta Pixel does not cause the user's browser to load the c_user and m_page_voice cookies. If the user's browser has the c_user and m_page_voice cookies, it will already be loaded when the Meta**

> **Pixel is invoked. Cookies are stored within the browser when they are created, and in this case, these cookies would have been created when the user logged in to Facebook; not when the user visited a page with a Meta Pixel. The Meta Pixel only causes the browser to communicate with Facebook, at which point Facebook does something that is opaque to the visited website, which might include retrieving the value within its own cookies.**

As discussed above, I made no error. While I agree that the cookies, if present, are already present when the user visits the ufcfightpass.com website, I disagree with his statement that Zuffa does not transmit them, for the reasons discussed above.

> **d. 12(f)(c) goes on to state, "At all relevant times, the Meta Pixel on the user's computer has been configured to transmit the c_user and m_page_voice cookies with the user's Facebook ID directly to the Facebook server. Zuffa thus caused the user's browser to send the user's Facebook ID to the Meta server." This is incorrect for two reasons:**
>
> **(i) As described supra, it implies that it is always the case, for all users, and**
>
> **(ii) Neither Ms. Herold nor Zuffa can say how "the Meta Pixel" was configured "at all relevant times," as neither had control over nor visibility to how the Meta Pixel worked at all relevant times. It was entirely under Meta's control what the Meta Pixel did, at all times. Other than contemporaneous evidence at a particular time, there is no way to say with certainty what the pixel caused to happen.**

Again, I made no error, for the same reasons discussed above. Mr. Schnell misrepresents my actual testimony. While it is technically true that Zuffa would not have directly observed the data transmissions, Zuffa should have known they were likely to occur, based on Meta's developer documentation. Moreover, they certainly had the technical capability to identify these problems if they had performed any quality assurance directed to PII transmission.

> **e. 12(g) states, "Meta stored and processed the data collected from the UFC Fight Pass subscriber to track online activities as established by the Meta Pixel and, for those periods it was in use, the Conversions API." In this subparagraph, Ms. Herold purports to have knowledge of what Facebook did (to a technical certainty), over a specific time period. All of the actions Ms. Herold states Facebook takes in this subparagraph happens completely within the Facebook servers. Ms. Herold has shown no scientific evidence as to what Facebook does with these data to which she refers. Additionally, it is unclear exactly to which data she does refer, considering the incorrect and impossible tracking of data she claims is collected, as described supra.**

Again, I made no error, for the same reasons discussed above. In any event, testimony from Meta corroborates most, if not all, of my testimony.

I declare under the penalty of perjury that the above is true.

Date: January 29, 2024

DocuSigned by:
Rebecca Herold
E25913437F094D9...

Rebecca Herold